

# 3-MANIFOLD DIAGRAMS AND NP VS #P

GORJAN ALAGIC AND CATHARINE LO

**ABSTRACT.** In computational complexity, a significant amount of useful theory is built on a foundation of widely-believed conjectures about the separation of complexity classes, the most famous of which is  $P \neq NP$ . In this work, we examine the consequences of one such conjecture on the combinatorics of 3-manifold diagrams. We use basic tools from quantum computation to give a simple (and unconditional) proof that the Witten-Reshetikhin-Turaev invariant of 3-manifolds is #P-hard to calculate. We then use this fact to show that, if  $NP \neq \#P$ , then there exist infinitely many 3-manifold diagrams which cannot be made logarithmically “thin” (relative to their overall size) except perhaps by an exponentially large number of local moves. The latter theorem is an analogue of a result of Freedman for the Jones Polynomial.

## 1. INTRODUCTION

**1.1. Complexity and low-dimensional topology.** In computational complexity, a significant amount of useful theory is built on a foundation of widely believed conjectures about the separation of complexity classes. The most famous example is the conjecture  $P \neq NP$ . Informally, it says the following: checking if an assignment of variables to a boolean formula evaluates to true, is significantly easier than finding such an assignment. Besides the well-known  $P$  and  $NP$ , another class of interest is  $\#P$ , which captures the difficulty of counting, e.g., the number of satisfying assignments to a boolean formula. Each of these three satisfiability problems (checking, finding, and counting) completely captures the power of the corresponding class (i.e., it is “hard” for that class). From this, one easily concludes that  $P \subseteq NP \subseteq \#P^1$ . Both containments are believed to be strict. Computational complexity theorists have a significant amount of confidence in the truth of these conjectures; this confidence rests on a large amount of theoretical work, as well as decades of practical experience. Indeed, NP-hard problems are of great practical interest (e.g., truck route planning) and have been the subject of decades of algorithm research and actual programming taking place in the real world. Still, the best algorithms we know today are about as fast as the obvious approach of checking every possibility, which takes time exponential in the input size. The problems in the class  $P$ , on the other hand, can be solved in polynomial time – and the polynomial is often of such low degree that the algorithms are quite practical. Despite the lack of formal proof for  $P \neq NP$  and many other separation conjectures, the surrounding theoretical work has had a significant impact on computer science, both theoretically and practically. This impact has extended to certain areas of mathematics and physics as well; some well-known examples in the last decade include work on geometric complexity theory and representation theory [32, 33], as well as important new insights in quantum computation [1] and condensed matter systems [10].

In low-dimensional topology, complexity theory has a natural role to play in classifying the difficulty of performing computations about topological spaces and their combinatorial representations. For instance, classifying compact orientable surfaces based on their triangulations is a problem in  $P$  – one simply calculates the Euler characteristic [18]. The problem of determining if a given knot is the unknot is known to be in both  $NP$  and  $coNP$  [11]. The difficulty of calculating some link invariants (such as the Jones Polynomial) is known to be much greater: it is  $\#P$ -hard [17]. By asking for approximations of these invariants (rather than the exact value), the complexity can become much more reasonable: the Jones Polynomial becomes tractable on quantum computers [8], while other link invariants become tractable in classical (i.e., non-quantum) polynomial time [12, 2, 14]. Unfortunately, these approximations are unlikely to be useful.

In this work, following ideas of M. Freedman [7, 4], we apply basic complexity theory to low-dimensional topology in a slightly different way. Freedman assumes a standard conjecture from complexity theory,

<sup>1</sup>Formally,  $P$  and  $NP$  are decision classes (i.e., testing membership in a set) while  $\#P$  is a counting class (i.e., calculating some integer-valued function). Thus, strictly speaking, writing  $NP \subseteq \#P$  is a type error. Nonetheless, it is clear what this means informally: if you know how to count the number of satisfying assignments, then you also know if it’s positive! One can also make formal sense of this via oracles, e.g., by writing  $NP \subseteq P^{\#P}$ .

namely  $\text{NP} \neq \#P$ , and couples it with the previously known fact that the Jones Polynomial is  $\#P$ -hard. He then shows that, if all link diagrams can be transformed to particularly “thin” diagrams with a polynomial number of local moves, then this would imply the existence of a polynomial-time verification of the value of their Jones Polynomial. Polynomial-time verification implies membership in  $\text{NP}$ , and (by  $\#P$ -hardness), this puts all of  $\#P$  into  $\text{NP}$ . It follows that some diagrams without this property exist, which turns out to be an interesting observation that Freedman believes is not provable with known methods in low-dimensional topology.

**1.2. The present work.** Our main result is an analogue of Freedman’s result in the case of 3-manifolds. Before getting to that result, we first show that the Witten-Reshetikhin-Turaev invariant of 3-manifolds is  $\#P$ -hard to approximate with exponentially small error. We assume that the input manifold is specified via a Heegaard splitting, i.e. a pair  $(g, \alpha)$  where  $g > 0$  is an integer and  $\alpha$  is an element of the mapping class group  $\text{MCG}(\Sigma_g)$  of the genus- $g$  surface. Recall that  $\text{MCG}(\Sigma_g)$  is finitely-generated, which allows for a combinatorial description of the map  $\alpha$ . We denote the manifold formed by gluing two  $g$ -handlebodies along the gluing map  $\alpha$  by  $M_{g, \alpha}$ .

**Theorem 1.1.** *The following problem is  $\#P$ -hard: given a list of generators  $w_1, \dots, w_n$  of  $\text{MCG}(\Sigma_g)$ , output a number  $r$  such that  $|r - \text{WRT}(M_{g, w_1 w_2 \dots w_n})| < \mathcal{D}^{1-g}/2^{g+1}$ , where  $\mathcal{D}$  is the total quantum dimension.*

In particular, calculating WRT exactly is also  $\#P$ -hard. The main tools in the proof are the Solovay-Kitaev theorem [5], which is standard in quantum computation literature, and a density theorem for WRT representations of mapping class groups, due to Larsen, Freedman and Wang [9, Theorem 6.2]. While the above statement is specific to the Fibonacci variant of the WRT, a similar fact (with slightly different bounds on the error) holds for all other variants of the WRT to which the density results of Larsen, Freedman and Wang apply.

A pair of Heegaard splittings  $(g, \alpha)$  and  $(g', \alpha')$  which describe homeomorphic 3-manifolds are said to be equivalent. Such a pair differs by a finite sequence of (geometrically local) combinatorial moves: a stabilization move which can increase or decrease the genus by one, and a handle-slide move which only affects the word [27]. The length of this sequence is denoted  $\text{dist}((g, \alpha), (g', \alpha'))$  is unknown in general; however, we can use Theorem 1.1 and the conjecture  $\#P \neq \text{NP}$  to give some interesting constraints on its scaling. We show that there exist infinitely many Heegaard splittings which cannot be transformed into a splitting with a genus which is much smaller than the size of the original splitting, unless one is allowed to make an exponentially large number of local moves. More precisely, we prove the following theorem.

**Theorem 1.2.** *Assume  $P^{\#P} \neq \text{NP}$ . Given any two polynomials  $p$  and  $q$ , there exists an infinite family of Heegaard splittings  $(g, \alpha)$  such that any  $(g', \alpha')$  equivalent to  $(g, \alpha)$  satisfies  $g' < \log(q(g + |\alpha|))$  unless  $\text{dist}((g, \alpha), (g', \alpha')) > p(g + |\alpha|)$ .*

We remark that this result holds even if we extend the above equivalence relation on Heegaard splittings by adding moves which disrupt homeomorphism type but leave some WRT invariant from Theorem 1.1 unchanged.

**1.3. Related results.** In 1989 and 1991, Witten, Reshetikhin and Turaev [24, 31] described invariants of 3-manifolds closely related to the Jones polynomial; these are precisely the Witten-Reshetikhin-Turaev invariants discussed above. Kirby and Melvin [13] later derived a formula for some WRT invariants as sums over link polynomials associated to certain quantum groups. Consequently, Freedman showed that the computation of the WRT invariant at the third root of unity has a polynomial time algorithm, while Kirby and Melvin [14] showed that evaluating the WRT invariant exactly at the fourth root of unity is  $\text{NP}$ -hard. In fact, their proof can also be used to show that the same problem is  $\#P$ -hard. In this paper, we extend this to show that computing WRT invariant is still  $\#P$ -hard for almost all choices of root of unity.

Based on previous results that evaluation of the Jones polynomial is  $\#P$ -hard [32, 33, 28], Freedman showed that there exist link diagrams  $L$  such that, if another diagram  $L'$  can be obtained from  $L$  by a polynomial number of Reidemeister moves (plus a particular Dehn surgery move,) then there is a logarithmic lower bound for the girth of  $L'$  [7]. Freedman et al [4] expanded on this work using more subtle separation axioms, this time for quantum complexity classes. Our result is an analogue of Freedman’s original paper, for the case of 3-manifolds.

**1.4. Organization.** The paper is organized as follows. The next two sections will provide important (but more-or-less known) material in 3-manifold topology and computational complexity. The goal of these sections is to make the result more accessible to researchers from both fields. In Section 4, we show that calculating the WRT invariant (or approximating it with exponentially small error) is #P-hard. In Section 5, we apply this fact to show the main result, namely Theorem 1.2.

## 2. 3-MANIFOLDS AND QUANTUM INVARIANTS

**2.1. 3-manifolds, Heegaard splittings, and invariance moves.** A manifold is a smooth topological space which locally looks like Euclidean space of a particular dimension. In this work, we will consider a particularly simple case of 3-manifolds; these are compact, connected Hausdorff spaces, each point of which has a neighborhood homeomorphic to  $\mathbb{R}^3$  [22]. Among the simplest examples are the three-sphere  $S^3$  and the three-torus  $T^3 = S^1 \times S^1 \times S^1$ . The natural notion of equivalence for 3-manifolds is homeomorphism; we write  $M \cong N$  to denote the fact that  $M$  and  $N$  are homeomorphic manifolds. The classification of 3-manifolds up to homeomorphism is a traditional question considered by topologists, and resolved in famous recent works on geometrization [29, 16]. In parallel, many invariants of 3-manifolds have been proposed; such invariants assign a number to each 3-manifold, with homeomorphic 3-manifolds getting the same number. Among the more famous examples are the quantum invariants, including the Turaev-Viro (TV) [30] and Witten-Reshetikhin-Turaev (WRT) [24, 31] invariants.

In order to do computations, we will make use of a well-known combinatorial description of 3-manifolds. Let  $\Sigma_g$  denote the compact orientable surface of genus  $g$ , and recall that the union of  $\Sigma_g$  with its interior is called a handlebody. Given two handlebodies  $A$  and  $B$  of equal genus, and a homeomorphism  $f : \Sigma_g \rightarrow \Sigma_g$ , we can form the quotient space  $M = A \sqcup_f B$  by identifying the surfaces of  $A$  and  $B$  via the gluing map  $f$ . It's easy to check that the resulting space is a compact 3-manifold. It is a theorem that any compact 3-manifold admits a description of this form, i.e., as a pair  $(g, f)$  where  $f$  is an element of the mapping class group  $\text{MCG}(\Sigma_g)$ . The group  $\text{MCG}(\Sigma_g)$  turns out to be finitely generated; the generators are Dehn twists about the  $3g - 1$  canonical curves shown in Figure 1, which we denote by  $w_1, w_2, \dots, w_{3g-1}$ , ordered from left to right. We thus arrive at a purely combinatorial description of any 3-manifold, as a pair  $(g, \alpha)$  where  $g$  is a positive integer and  $\alpha$  is a finite sequence of integers corresponding to Dehn twists. We will refer to such a pair as a Heegaard splitting, and write  $M_{g,\alpha}$  for the corresponding homeomorphism class of 3-manifolds. For the purposes of discussing the scaling of computational problems, we also define the “input length” of a Heegaard splitting as the genus plus the number of generators in the word:  $|(g, \alpha)| := g + |\alpha|$ .

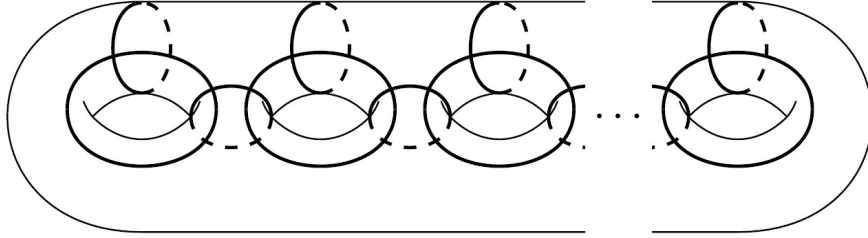


Figure 1: Dehn twist generators

It is natural to ask how one can modify a Heegaard splitting while leaving the corresponding 3-manifold homeomorphism class unchanged. Just as with knot diagrams and triangulations, there's a finite set of “invariance moves” on Heegaard splittings [27]. We now describe these moves. In particular, we give a way to present each move in a purely combinatorial fashion, and show how to efficiently check whether a proposed move is valid for a given Heegaard splitting. This aspect of these moves will be critical in the proof of our main theorem.

The first move is the “handle-slide” and maps  $(g, x) \rightarrow (g, yxz)$  where  $y$  and  $z$  are self-homeomorphisms of  $\Sigma_g$  that extend to self-homeomorphisms of the handlebody. In other words, both  $y$  and  $z$  are elements of the so-called handlebody subgroup  $\text{MCG}^+(g) \leq \text{MCG}(\Sigma_g)$ . Handle-slide moves are presented via a description of  $y$  and  $z$  as words in the Dehn twist generators of  $\text{MCG}(\Sigma_g)$ . To check the validity of a proposed handle-slide move, one must verify that both words belong to the handlebody subgroup.

**Theorem 2.1.** [26, Theorem 6.4] *The following problem admits a polynomial-time algorithm: given a sequence of Dehn twist generators describing an element  $x \in \text{MCG}(\Sigma_g)$ , determine whether  $x \in \text{MCG}^+(g)$ .*

The second move is “stabilization,” and it allows us to increase (or, under certain conditions, decrease) the genus. There’s a trivial embedding

$$\tau : \text{MCG}(\Sigma_g) \hookrightarrow \text{MCG}(\Sigma_{g+1})$$

defined by sending the  $j$ th generator of  $\text{MCG}(\Sigma_g)$  to the  $j$ th generator of  $\text{MCG}(\Sigma_{g+1})$  for all  $j \leq 3g - 1$ . Consider also the genus-one Heegaard splitting of the three-sphere defined by  $(1, aba^{-1})$ , where  $a$  and  $b$  denote the two Dehn twist generators of  $\text{MCG}(\Sigma_1)$ . The stabilization move is then defined by

$$(g, x) \rightarrow (g + 1, \tau(x)w_{3g-1}w_{3g-2}w_{3g-1}^{-1}).$$

This corresponds to taking the connected sum of  $M_{g,x}$  with the three-sphere. The stabilization move has an inverse move, which is known as destabilization; it can only be applied if we can “undo” a connected sum with the three-sphere. More precisely, the word must terminate in  $w_{3g}w_{3g-1}w_{3g}^{-1}$ , and the generators  $w_{3g}$  and  $w_{3g-1}$  may not appear anywhere else in the word.<sup>2</sup> As with handle-slides, we will require a way to present stabilization and destabilization moves in a polynomial-time verifiable manner. Presentation is straightforward: a single bit is sufficient: 1 to stabilize, 0 to destabilize. Stabilization is always allowed, and destabilization of  $(g, \alpha)$  is only allowed if the word  $\alpha$  satisfies the conditions given above, which can be checked by straightforward string comparisons.<sup>3</sup>

It’s not hard to check that both stabilization and handle-slide leave the corresponding 3-manifold homeomorphism type fixed. It is a theorem that finite-length sequences of these moves are sufficiently powerful to describe all equivalences between Heegaard splittings. Before stating this theorem, it will be useful to precisely set down the notion of distance between Heegaard splittings. First, we define a length  $|\cdot|$  for moves. A handle-slide  $(g, x) \rightarrow (g, yxz)$  is described by two words  $\alpha_y$  and  $\alpha_z$  in the Dehn twist generators of  $\text{MCG}(\Sigma_g)$ ; we define the length of such a move to be  $|\alpha_y| + |\alpha_z|$ . A stabilization move is described by a single bit which determines if the genus should increase or decrease; the length of a stabilization move is thus always one. The length  $|s|$  of a sequence  $s$  of handle-slides and stabilization moves is simply the sum of the lengths of all the moves in the sequence. Now we are ready to define a distance between a pair  $(g, \alpha)$  and  $(g', \alpha')$  of Heegaard splittings:

$$\mathbf{dist}((g, \alpha), (g', \alpha')) := \min\{|s| : s \text{ is a sequence of moves with } s(g, \alpha) = (g', \alpha')\}.$$

If no sequence of moves suffices, then the distance is defined to be infinite. The distinction between finite and infinite distance captures the notion of 3-manifold homeomorphism.

**Theorem 2.2.** [27, 23] *Let  $(g, \alpha)$  and  $(g', \alpha')$  be two Heegaard splittings. Then  $\mathbf{dist}((g, \alpha), (g', \alpha'))$  is finite if and only if the corresponding 3-manifolds  $M_{g,\alpha}$  and  $M_{g',\alpha'}$  are homeomorphic.*

**2.2. Quantum invariants of 3-manifolds.** We now define the WRT invariant of a 3-manifold presented as a Heegaard splitting. For our purposes, it will be convenient to define the invariant in terms of a particular representation of the mapping class group. We will define a representation  $\rho_{\mathcal{C},g}$  of  $\text{MCG}(\Sigma_g)$ , where  $\mathcal{C}$  is a choice of multiplicity-free unitary modular tensor category. The detailed theory of such categories will not be crucial to our presentation; it is, of course, quite important for a proof that the final quantity below is indeed an invariant of 3-manifolds. For us, it will suffice to know that  $\mathcal{C}$  encapsulates the following pieces of data:

- (1) a finite set  $\Sigma$  of  $m$  “labels”; each label  $j \in \Sigma$  is associated with a dual label  $j^* \in \Sigma$ , and there is a distinguished “trivial” self-dual label  $0$ ;
- (2) a list  $d : \Sigma \rightarrow \mathbb{C}$  of “dimensions” for each label;
- (3) a finite set  $O \subset \Sigma \times \Sigma \times \Sigma$  of “fusion rules”;
- (4) an “R-move” tensor  $R_i^{jk}$  which associates each triple from  $\Sigma$  to a complex number;
- (5) a unitary “F-move” tensor  $F_{ijk}^{lmn}$  which associates each sextuple from  $\Sigma$  to a complex number.

The formal definition of a multiplicity-free unitary modular tensor category puts various constraints on the above data, e.g.,  $R_i^{jk} = 0$  unless  $(i, j, k) \in O$ . One may think of the above data as describing an analogue

<sup>2</sup>It is known that the genus-one Heegaard splittings of the three-sphere are related only by isotopies and handle-slides [25, Theorem 3.7]. It thus suffices to consider the particular choice of stabilization and destabilization move we chose.

<sup>3</sup>It might seem that we should also allow destabilization if there is another word  $\alpha'$  which satisfies the conditions described above, and is equivalent to  $\alpha$ , i.e.  $\alpha\alpha' = 1$ . This is actually not necessary: since 1 is obviously in the handlebody subgroup, the transformation  $\alpha \mapsto \alpha'$  is a valid handle-slide.

of a representation ring, where the labels correspond to irreducible representations, the notion of dual and dimension have the obvious meaning, the fusion rules correspond to the Clebsch-Gordan rule, etc. In general, the five pieces of data above always determine two additional quantities which we will require. These are the “total dimension”  $\mathcal{D}$  and the “S-move” tensor, defined by

$$(1) \quad \mathcal{D} = \sqrt{\sum_{j \in \Sigma} d_j} \quad \mathcal{D} S_{jk}^i = \sum_{l: (j, k^*, l) \in O} \frac{d_l}{\sqrt{d_i}} F_{lj^*j}^{ik^*k} R_l^{kj^*} R_{l^*}^{jk^*}.$$

To define the representation  $\rho_{\mathcal{C},g}$ , we first define the underlying vector space. Decompose  $\Sigma_g$  into three-punctured spheres or “pants” as shown in the figure below; we will refer to this as the standard pants decomposition of  $\Sigma_g$ . Dual to such a pants decomposition is a trivalent graph  $\Gamma$  called the spine. The spine has one vertex for every pants in the decomposition, and one edge for each meeting between two pants. We may then assign labels from  $\Sigma$  to the edges of  $\Gamma$ . Such a labeling is called fusion-consistent if, for every vertex  $v$  of  $\Gamma$ , the set of edges of  $v$  is an element of the fusion rules  $O$ . We define the Hilbert space  $\mathcal{H}_{\mathcal{C},g}$  to be the orthonormal span of vectors  $|l\rangle$ , one for every fusion-consistent labeling  $l$  of the edges of  $\Gamma$ .

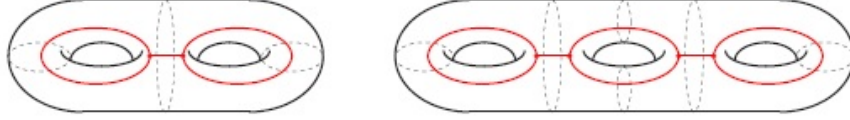


Figure 2: Pants decomposition of a genus-2 handlebody and genus-3 handlebody

Next, we define the action of the generators of  $\text{MCG}(\Sigma_g)$  on  $\mathcal{H}_{\mathcal{C},g}$ , which will define  $\rho_{\mathcal{C},g}$  completely. Let  $n$  denote the number of edges of  $\Gamma$ . The space  $\mathcal{H}_{\mathcal{C},g}$  embeds into  $(\mathbb{C}^m)^{\otimes n}$  (i.e., the space of all possible labelings of the edges, consistent or not) in the obvious way. The F-move and the R-move can be viewed as linear operators on either space, as shown in the expressions below. Note that these operators act in a local way, in the sense that they are the identity on all but a constant ( $\leq 6$ ) number of tensor factors. In each expression below, the right-hand side is the image of a basis element of  $\mathcal{H}_{\mathcal{C},g}$  under one such linear operator, and is again clearly an element of  $\mathcal{H}_{\mathcal{C},g}$ . It turns out that this new element can be suitably interpreted as an orthonormal basis element in another (isomorphic) Hilbert space, which corresponds to a different pants decomposition of  $\Sigma_g$ , as shown on the left-hand side.

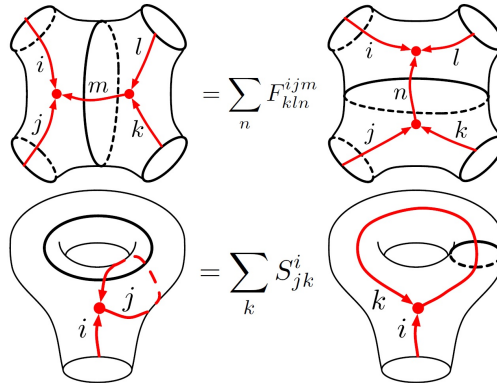


Figure 3: F and S move expressions

Given a canonical curve  $\gamma$  on  $\Sigma_g$ , let  $\sigma_\gamma$  denote the corresponding Dehn twist. First, suppose that  $\gamma$  is a cut in the standard pants decomposition, and let  $e_\gamma$  denote the corresponding edge of the spine  $\Gamma$ . The action of  $\sigma_\gamma$  on a labeling  $l$  depends on the relevant label  $i := l(e_\gamma)$ , as follows:

$$(2) \quad \rho_{\mathcal{C},g}(\sigma_\gamma) : |l\rangle \mapsto e^{R_0^{ii^*}} |l\rangle.$$

Now suppose  $\gamma$  is a canonical curve but not a cut in the standard pants decomposition. Using earlier expressions, one easily checks that at most one F-move and one S-move suffice to change the standard pants decomposition to a pants decomposition where  $\gamma$  is a cut. In that basis (now consisting of labelings of a different spine),  $\sigma_\gamma$  acts as in (2).



Finally, we define the WRT invariant as a particular, scaled matrix entry of the representation  $\rho_{\mathcal{C},g}$  [21]. Let  $|0\rangle \in \mathcal{H}_{\mathcal{C},g}$  denote the basis vector corresponding to the labeling where each edge of the spine carries the trivial label 0.

**Definition 1.** *Let  $(g, \alpha)$  be a Heegaard splitting. The Witten-Reshetikhin-Turaev invariant of  $(g, \alpha)$  is defined to be*

$$\text{WRT}(g, \alpha) = \mathcal{D}^{g-1} \langle 0 | \rho_g(\alpha) | 0 \rangle.$$

The central fact is that  $\text{WRT}(g, \alpha)$  depends only on the homeomorphism type of  $M_{g,\alpha}$ .

**Theorem 2.3.** *Let  $(g, \alpha)$  and  $(g', \alpha')$  be Heegaard splittings corresponding to homeomorphic 3-manifolds, i.e., such that  $M_{g,\alpha} \cong M_{g',\alpha'}$ . Then  $\text{WRT}(g, \alpha) = \text{WRT}(g', \alpha')$ .*

The proof proceeds by establishing the invariance of WRT under both the stabilization and the handle-slide moves described above. Refer to [34] and [24] for a complete proof. Taken together with Theorem 2.2, this means that WRT is indeed an invariant of 3-manifolds.

Our proofs will make use of the following fact about certain variants of the WRT.

**Theorem 2.4** (Density of Fibonacci representations). *Except when  $g + n = 1$ ,  $\rho_{g,n}(P_{g,n})$  is dense in  $\text{PU}(\dim \mathcal{H}_{\Sigma_{g,n}})$ . [9, Theorem 6.2]*

For concreteness, we briefly describe the simplest choice for the category  $\mathcal{C}$ , for which the above theorem and all of our results hold. This is the so-called Fibonacci category, and is defined with the following data [12, 2].

- (1) label set  $\Sigma = \{0, 1\}$ , with  $1^* = 1$ ;
- (2) dimensions  $d_0 = 1$  and  $d_1 = (1 + \sqrt{5})/2$ ;
- (3) fusion rules  $O = \{(a, b, c) \in \Sigma^3 : a + b + c \neq 1\}$ ;
- (4) R-tensor defined by  $R_0^{00} = 0$  and  $R_0^{11} = 3\pi i/5$ ;
- (5) F-tensor defined by

$$\begin{aligned} \begin{array}{c} 1 \quad 1 \\ \diagdown \quad \diagup \\ \bullet \\ \diagup \quad \diagdown \\ 1 \quad 1 \end{array} &= \frac{2}{1 + \sqrt{5}} \begin{array}{c} 1 \quad 1 \\ \diagdown \quad \diagup \\ \bullet \\ \diagup \quad \diagdown \\ 1 \quad 1 \end{array} + \sqrt{\frac{2}{1 + \sqrt{5}}} \begin{array}{c} 1 \quad 1 \\ \diagdown \quad \diagup \\ \bullet \\ \diagup \quad \diagdown \\ 1 \quad 1 \end{array} \\ \begin{array}{c} 1 \quad 1 \\ \diagdown \quad \diagup \\ \bullet \\ \diagup \quad \diagdown \\ 1 \quad 1 \end{array} &= \sqrt{\frac{2}{1 + \sqrt{5}}} \begin{array}{c} 1 \quad 1 \\ \diagdown \quad \diagup \\ \bullet \\ \diagup \quad \diagdown \\ 1 \quad 1 \end{array} + \frac{-2}{1 + \sqrt{5}} \begin{array}{c} 1 \quad 1 \\ \diagdown \quad \diagup \\ \bullet \\ \diagup \quad \diagdown \\ 1 \quad 1 \end{array} \end{aligned}$$

It's not hard to check that the above values determine the R-tensor and F-tensor fully: the remaining values are forced by the fusion rules (and are either zero or one). Using equation (1), we see that the total dimension satisfies  $\mathcal{D}^2 = (5 + \sqrt{5})/2$  and that the S-tensor is defined by

$$\begin{aligned} \mathcal{D}S_{00}^0 &= 1 & \mathcal{D}S_{10}^0 &= \mathcal{D}S_{01}^0 = \frac{1 + \sqrt{5}}{2} \\ \mathcal{D}S_{11}^0 &= 1 + \frac{1 + \sqrt{5}}{2} e^{i4\pi/5} & \mathcal{D}S_{11}^1 &= \sqrt{\frac{1 + \sqrt{5}}{2}} (1 - e^{i4\pi/5}). \end{aligned}$$

### 3. BASIC COMPUTATIONAL COMPLEXITY AND QUANTUM CIRCUITS

**3.1. P, NP, and #P.** Computational complexity attempts to classify problems according to the number of basic computation steps<sup>4</sup> required to solve them, expressed as a function of the input size. In the simplest case, a problem is described by a subset  $L$  of the set  $\{0, 1\}^*$  of all bitstrings, and the task is to decide if a given input string is in  $L$  or not. An important set of examples relates to satisfiability of boolean formulas. Recall that a boolean formula is an expression involving a finite number of input variables (literals), NOTs

<sup>4</sup>The notion of computation time can be fully formalized using Turing Machines. It is sufficient to think about writing a computer program for the task, and considering the total number of basic instructions (e.g., additions or multiplications) the program must execute on a given input.

(negations), ANDs (conjunctions), and ORs (disjunctions). In this work, we will assume that all formulas are 3CNF, i.e., a conjunction of clauses where each clause is a disjunction of three literals (negated or not). We will also assume that we have fixed some particular encoding of 3CNF formulas as bitstrings. The only thing we require about this encoding is that it is linear, i.e., that the length of the bitstring and the length of the formula are related by at most a constant factor; this is straightforward to accomplish.

The first relevant problem in satisfiability is assignment checking: given a 3CNF boolean formula  $\varphi$  and a setting  $x$  of its input variables to values in  $\{0, 1\}$ , does  $\varphi(x)$  evaluate to 0 (false) or 1 (true)? This can be done in a number of computation steps which is polynomial (in fact, linear) in the length of the description of  $\varphi$  and  $x$  as bitstrings. We thus say that this problem is in the class  $P$ , consisting of all problems which can be solved in polynomial time.

The next relevant problem is determining satisfiability (3SAT): given a 3CNF boolean formula  $\varphi$ , does there exist a setting  $x$  of its inputs such that  $\varphi(x) = 1$ , or not? A trivial but useful observation is that, if someone provides you with an  $x$  (a “proof”) such that  $\varphi(x) = 1$ , then the problem of verifying this fact is in  $P$ . This means that 3SAT falls into the class NP of problems whose positive solutions are verifiable in polynomial time. In fact, by the famous Cook-Levin theorem [3, 19], 3SAT is also “hard” for the class NP, i.e., any other problem  $L$  in NP can be reduced to solving 3SAT. More precisely, there is a polynomial time algorithm  $A_L$  such that, for any input  $x$ ,  $x \in L$  if and only if  $A(x) \in 3SAT$ . In particular, an algorithm for 3SAT can also be used to solve any other problem in NP, with at most a polynomial number of extra steps. But how do we directly attack 3SAT itself? The obvious approach is to simply try all possible assignments, of which there are exponentially many. If one can do significantly better is one of the biggest open questions in science: is  $P = NP$ ? Of course, the conjectured state of affairs is  $P \neq NP$ .

The third relevant problem counts satisfying assignments ( $\#SAT$ ): given a 3CNF boolean formula  $\varphi$ , how many assignments  $x$  satisfy  $\varphi(x) = 1$ ? This problem is contained in (and is hard for) the class  $\#P$ . This class demands that the output to the algorithm is a number  $m$  such that there exist exactly  $m$  distinct proofs, each of which is polynomial-time checkable; in the case of  $\#SAT$ , these proofs are the satisfying assignments themselves, and the polynomial-time checker is the first algorithm discussed above. Clearly,  $\#SAT$  is at least as hard as 3SAT, so  $NP \subseteq \#P$ . It is a widely-believed conjecture that the containment is strict, i.e. that  $NP \neq \#P$ .<sup>5</sup>

**3.2. Quantum Circuits.** Recall that a boolean circuit consists of wires and gates; each wire carries a bit, while the gates perform local boolean operations. We say that the boolean circuit implements the boolean function defined by the composition of these operations. The boolean circuit is a very useful abstraction for thinking about computation with classical, digital computers. An analogous abstraction can also be defined for quantum-mechanical devices for computation: a quantum circuit. Quantum circuits also consist of wires and gates. Each wire now carries a qubit state, i.e., a unit vector in the space  $\mathbb{C}^2$  equipped with a preferred basis  $\{|0\rangle, |1\rangle\}$ , corresponding to the values of a classical bit. Each gate represents a unitary operator acting on a small number of qubits, and leaving the remaining qubits fixed. We say that the circuit implements the unitary operator defined by the composition of these local gates. It is important to note that, unlike with classical boolean circuits, in a quantum circuit the total number of qubits never changes, and the entire operation is invertible; indeed, violating either requirement would imply that the total circuit is no longer unitary.

It is standard to fix a small gate set and define all circuits using this set. We will use the set  $\{H, T\}$ , where

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad \text{and} \quad T : |x, y, z\rangle \rightarrow |x, y, z \oplus xy\rangle,$$

i.e.  $H$  is the Hadamard operator and  $T$  is the controlled-controlled-NOT gate (also called the Toffoli gate.) It is straightforward to check that these gates are unitary. They are also universal for quantum computation.<sup>6</sup>

Starting with the formalism of quantum circuits, one may define a model of quantum computation (see [20] for details.) It is natural to ask if this model of computation depends on the choice of gate set in some way. The Solovay-Kitaev theorem says that the answer is no: all universal gate sets define the same model of

<sup>5</sup>Technically, NP and  $\#P$  are incomparable because NP contains decision problems, while  $\#P$  contains counting problems. Nonetheless, using polynomial-time reduction algorithms, one can make a sensible statement of NP vs  $\#P$  which agrees with the intuition we discussed here.

<sup>6</sup>Technically, they are universal for quantum circuits with real matrix entries, but this turns out to be sufficient.

efficient quantum computation. More precisely, any universal gate set can simulate any other, with arbitrary operator-norm precision and polylogarithmic overhead.

**Theorem 3.1** (Solovay-Kitaev [20]). *Let  $S$  be a finite set of unitary operators which is closed under inverses and spans a dense subset of  $SU(d)$ . Then for any  $U \in SU(d)$  and any  $\varepsilon > 0$ , there exists a composition  $U' = G_1 \circ G_2 \cdots \circ G_m$  of operators from  $S$  such that  $\|U' - U\| < \varepsilon$  and  $m = \log^2(1/\varepsilon)$ .*

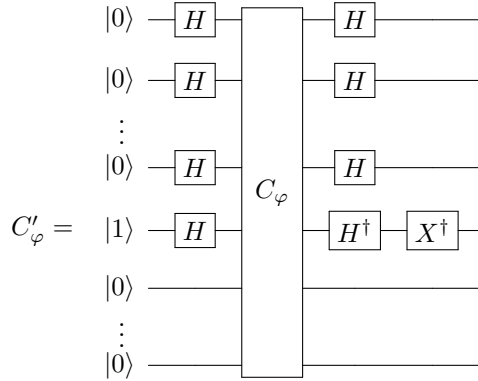
**3.3. Calculating a matrix entry of a quantum circuit is #P-hard.** We will require the following straightforward result from quantum computation; it appears to be folklore in that community. In further discussions, it will be important to distinguish between two meanings of “quantum circuit”: one is the description of the circuit, which is just a list of integers describing the number of qubits and the position of each gate; the other is the actual unitary operator implemented by the circuit. If the relevant meaning is not clear from context, we will say so explicitly.

**Problem 1.** Given a description of a quantum circuit  $C$  over the gate set  $\{H, T\}$ , output a number  $r$  such that

$$|r - \langle 0 \cdots 0 | C | 0 \cdots 0 \rangle| < \frac{1}{2^n}.$$

**Theorem 3.2.** *Problem 1 is #P-hard.*

*Proof.* We will prove the theorem by reducing #SAT to Problem 1. Let  $\varphi : \{0, 1\}^n \rightarrow \{0, 1\}$  be a 3-CNF formula. We first create the reversible circuit  $C_\varphi : (x, 0) \mapsto (x, \varphi(x))$  by replacing the classical gates  $\{\neg, \wedge, \vee\}$  with their corresponding Toffoli gate sequences, using ancillas if necessary [20]. Then, there is a classical circuit, with  $a$  ancillas of size  $\sim |\varphi|$  that computes  $\varphi$  given by [6]



where  $X$  is the Pauli- $X$  gate, and  $H$  is the Hadamard gate.

Through this circuit,

$$\begin{aligned} |0\rangle^n |1\rangle^a |0\rangle^a &\mapsto H^{\otimes n+1} \otimes \mathbb{1}^a |0\rangle^n |1\rangle^a |0\rangle^a \\ &= \frac{1}{2^{n/2}} \sum_x |x\rangle^n |-\rangle^1 |0\rangle^a \\ &\mapsto \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} |x\rangle^n |\varphi(x) \oplus -\rangle^1 |0\rangle^a, \text{ where } \oplus \text{ is addition modulo 2} \\ &= \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} (-1)^{\varphi(x)} |x\rangle^n |-\rangle^1 |0\rangle^a \\ &\mapsto \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} (-1)^{\varphi(x)} H^{\otimes n} \otimes X^\dagger H^\dagger \otimes \mathbb{1} |x\rangle^n |-\rangle^1 |0\rangle^a \\ &= \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} (-1)^{\varphi(x)} H^{\otimes n} |x\rangle^n |0\rangle^1 |0\rangle^a \end{aligned}$$

Therefore the first matrix entry of the whole circuit is given by



$$\begin{aligned}
^{n+1+a} \langle 0 | \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} (-1)^{\varphi(x)} H^{\otimes n} |x\rangle |0\rangle^1 |0\rangle^a &= \frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{\varphi(x)} \sum_{y \in \{0,1\}^n} \langle y | x \rangle \\
&= \frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{\varphi(x)} \\
&= 1 - \frac{\#\varphi}{2^{n-1}}.
\end{aligned}$$

As such, if a quantum circuit gives an output  $r$  such that

$$|\langle 0^{\otimes n} | C | 0^{\otimes n} \rangle - r| < \frac{1}{2^n},$$

then

$$|\#\varphi - 2^{n-1}(1-r)| < \frac{1}{2}.$$

Since  $\varphi$  is a positive integer, we can calculate  $\#\varphi$  exactly from the output  $r$  by giving the closest integer to  $2^n(1-r)$ .  $\square$

#### 4. #P-HARDNESS OF WRT AND MANIFOLD DIAGRAMS

**4.1. Calculating the WRT invariant is #P-hard.** Our first result shows that approximating the WRT invariant to exponential accuracy is a #P-hard problem. The proof is essentially the exponential-accuracy version of the main theorem in [2]. The proof method is standard in quantum computation; the key ingredients are the Solovay-Kitaev theorem, the density theorem of Freedman, Larsen and Wang, and Theorem 3.2.

**Problem 2.** Given a sequence of generators  $w = (w_1, \dots, w_k)$  of  $\text{MCG}(\Sigma_g)$ , output a number  $r$  such that

$$|r - \text{WRT}(M_{g,w})| < \frac{\mathcal{D}^{1-g}}{2^{g+1}}.$$

**Theorem 4.1.** *Problem 2 is #P-hard.*

*Proof.* We want to reduce Problem 2 from Problem 3. To do this, given any quantum circuit  $C$ , we construct the Heegaard splitting such that  $\mathcal{D}^{1-g} \text{WRT}(g, \alpha)$  approximates  $\langle 0 | C | 0 \rangle$ , similar to [2]. As illustrated in Figure 4 below, we use one handle of a genus- $g$  handlebody to encode each qubit. Such a labelling is fusion-consistent, since the vertex  $v_{2i}$  (resp.  $v_{2i-1}$ ) has no 1's if  $z_i = 0$  (resp.  $z_{i-1} = 0$ ) and has two 1's if  $z_i = 1$  (resp.  $z_{i-1} = 1$ ). Then each labelling is mapped to an element in  $(\mathbb{C}^2)^{\otimes n}$  through the map

$$\iota : (\mathbb{C}^2)^{\otimes n} \hookrightarrow \mathcal{H}_{C,g}.$$

In particular, the state  $|0^g\rangle$  is mapped to  $|0\rangle \in \mathcal{H}_{C,g}$ . By definition,  $U(\mathcal{H}_{C,g})$  is a universal gate set [15], and  $n = g$ .

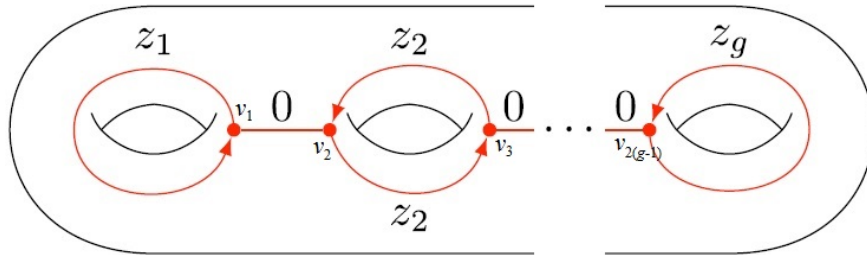


Figure 4: Encoding of a  $g$ -qubit state  $|z\rangle, z \in \{0,1\}^g$  into  $\mathcal{H}_{C,g}$  for the genus- $g$  handlebody

By Theorem 2.4, the set of representations  $\rho_{C,g}$  are dense in  $U(\mathcal{H}_{C,g})$ . Then for each  $C \in \iota(\mathbb{C}^2)^{\otimes n}$ , we can apply the Solovay-Kitaev theorem (Theorem 3.1) gate-by-gate with  $\varepsilon = 1/2^{g+1}$  on  $C$ , since we have constructed a labelling for  $C$ . Each gate  $C_j \in C$  is replaced with a sequence  $w_j$  of Dehn twists, such that

$|C_j - \rho(w_j)| < 1/|C|2^{g+1}$ . Then  $|C - \rho(w)| < 1/2^{g+1}$ , where  $w = w_1 w_2 \cdots w_{|C|} \in \text{MCG}(\Sigma_g)$ . Finally, note that for any operator  $A$ ,

$$|\langle 0|A|0\rangle|^2 = |\langle A^\dagger 0|0\rangle|^2 \leq |\langle A^\dagger|0\rangle|^2 \leq |A^\dagger|^2 = |A|^2.$$

Therefore,

$$|\langle 0|C|0\rangle - \langle 0|\rho_g(w)|0\rangle| = |\langle 0|C - \rho_g(w)|0\rangle| < |C - \rho_g(w)| < \frac{1}{2^{g+1}}.$$

Hence, if a black box that solves problem 2 gives an output  $r$  such that

$$|\langle 0|\rho_g(w)|0\rangle - \mathcal{D}^{1-g}r| < \frac{1}{2^{g+1}},$$

then by the triangle inequality,

$$|\langle 0|C|0\rangle - \mathcal{D}^{1-g}r| < \frac{1}{2^g}.$$

Since approximating  $\langle 0|C|0\rangle$  to  $1/2^g$  is  $\#P$ -hard by Theorem 3.2, Problem 2 is  $\#P$ -hard.  $\square$

Our main results will actually only need the fact that exact calculation of the WRT invariant is  $\#P$ -hard, which is an immediate corollary of the above theorem. Indeed, if one can exactly calculate WRT, then one can also satisfy the conditions of Theorem 4.1, which is at least as hard as any other problem in  $\#P$ .

**Problem 3.** Given a sequence of generators  $w = (w_1, \dots, w_k)$  of  $\text{MCG}(\Sigma_g)$ , output  $\text{WRT}(M_{g,w})$ .

**Corollary 4.1.** *Problem 3 is  $\#P$ -hard.*

**4.2. Implications for manifold diagrams.** We now prove our main result. We assume the widely accepted conjecture that  $\text{NP} \neq \#P$ , and prove the existence of an infinite family of peculiar Heegaard splittings. These splittings cannot be made logarithmically thin (as a function of their overall size), except possibly via an exponentially long sequence of moves. Recall that the input length  $|(g, \alpha)|$  of a Heegaard splitting  $(g, \alpha)$  in the hardness results above is simply the genus plus the length  $|\alpha|$  of the word  $\alpha$ .

**Theorem 4.2.** *Assume  $\text{NP} \neq \#P$ . Choose any two polynomials  $p$  and  $q$  with positive integer coefficients. Then there is an infinite family of Heegaard splittings  $(g, \alpha)$  with the following property:*

$$(3) \quad \text{if } M_{g', \alpha'} \cong M_{g, \alpha} \text{ then } g' > \log(q(g + |\alpha|)), \text{ unless } \mathbf{dist}((g, \alpha), (g', \alpha')) > p(g + |\alpha|).$$

*Proof.* We will assume that there exists a pair of polynomials  $p$  and  $q$  such that there are only finitely many Heegaard splittings  $(g, \alpha)$  satisfying property (3); our goal is to reach the conclusion that  $\#P \subset \text{NP}$ . To reach this conclusion, we will put Problem 3 (which is  $\#P$ -hard) into  $\text{NP}$ . We will do so via a standard complexity-theoretic method: prove the existence of a polynomial-length certificate, and give a polynomial-time algorithm for verifying the certificate. The certificate together with the verification algorithm will enable exact polynomial-time calculation of the WRT invariant.<sup>7</sup>

Proceeding with the aforementioned assumption, we see that there exists  $N > 0$  such that all  $(g, \alpha)$  satisfying  $|(g, \alpha)| \geq N$  violate property 3. In other words, for each such  $(g, \alpha)$ , there exists another Heegaard splitting  $(g', \alpha')$  satisfying

- (i)  $M_{g', \alpha'} \cong M_{g, \alpha}$ ,
- (ii)  $g' < \log q(g + |\alpha|)$ , and
- (iii)  $\mathbf{dist}((g', \alpha'), (g, \alpha)) < p(g + |\alpha|)$ .

For the remainder of the proof, let  $(g, \alpha)$  be an input Heegaard splitting, and let  $n := |(g, \alpha)| \geq N$  be its length. This is the input length to Problem 3, and the scaling of all relevant quantities (e.g., the certificate and the verification algorithm) will be measured as a function of  $n$ . By property (iii.), there exists a sequence  $\omega_{g, \alpha}$  of stabilization and handle-slide moves which describe how to transform  $(g, \alpha)$  into  $(g', \alpha')$  and which have a combined length which is polynomial in  $n$ . As described in Section 2.1, this means that  $\omega_{g, \alpha}$  has a string description which is also of length polynomial in  $n$ . This description of  $\omega_{g, \alpha}$  will be our certificate for exact calculation of  $\text{WRT}(M_{g, \alpha})$ .

<sup>7</sup>Recall that  $\text{NP}$  is technically a decision class, and any problem in  $\text{NP}$  thus must have a yes or no answer. So technically, we will put a  $\#P$ -hard problem into  $\text{FP}^{\text{NP}}$ , where  $\text{FP}$  denotes the class of polynomial-time computable functions. This is a relevant technical distinction in complexity theory, but is not particularly important in our setting.

We now describe the polynomial-time verification algorithm. It receives two inputs: a description of the Heegaard splitting  $(g, \alpha)$ , and an advice bitstring  $s$ . The task of the algorithm is to correctly output the exact value of the WRT invariant of  $M_{g, \alpha}$  when  $s$  is a valid certificate, as described above, and output “REJECT” otherwise.<sup>8</sup>

The algorithm proceeds in two stages. In the first stage, we verify that (i.) the advice string  $s$  describes a valid sequence  $\omega_{g, \alpha}$  of stabilization and handle-slide moves that can be applied to  $(g, \alpha)$ , and (ii.) after applying all the moves described in  $\omega_{g, \alpha}$ , we are left with some Heegaard splitting  $(g', \alpha')$  which satisfies  $g' < \log q(n)$ . To perform step (i.), we maintain a working description of a Heegaard splitting, starting with  $(g, \alpha)$ . Each stabilization move described by  $s$  can be verified in linear time: it either increases the genus (which we always accept), or it decreases the genus (which we accept if none of the generators in the working Heegaard splitting involve the last handle). Checking a handle-slide move is simply a matter of making sure that the given sequence of Dehn twists is really an element of the handlebody subgroup. This can be done in polynomial time via Theorem 2.1. Rewriting the working description to apply each move takes at most polynomial time as well. Step (ii.) is straightforward.

In the second stage of the algorithm, we calculate the WRT invariant of  $M_{g, \alpha}$  exactly. From the first stage, we have a new Heegaard splitting  $(g', \alpha')$  of polynomial length and logarithmic genus, and we have verified that  $M_{g, \alpha} \cong M_{g', \alpha'}$ . It thus suffices to calculate  $\text{WRT}(g', \alpha')$ , which can be done simply by matrix multiplication. Recall that by Definition 1,

$$\text{WRT}(g', \alpha') = \mathcal{D}^{g'-1} \langle 0 | \rho_{g'}(\alpha') | 0 \rangle,$$

where the representation  $\rho_{g'}$  has dimension which is exponential in the genus  $g'$ . Since  $g'$  is itself logarithmic in  $n$ , the dimension of  $\rho_{g'}$  is polynomial in  $n$ . We may write out  $\alpha' = \alpha'_1 \alpha'_2 \cdots \alpha'_m$  in terms of generators, so that

$$\rho_{g'}(\alpha') = \rho_{g'}(\alpha'_1) \rho_{g'}(\alpha'_2) \cdots \rho_{g'}(\alpha'_m)$$

is now a product of  $m$  matrices of polynomial dimension. The obvious matrix multiplication algorithm takes cubic time, and by property (iii.) above,  $m$  is polynomial in  $n$ . We can thus multiply all the above matrices and determine  $\rho_{g'}(\alpha')$  completely in time polynomial in  $n$ . It remains to simply look up a matrix entry of the resulting matrix, and scale it by  $\mathcal{D}^{g'-1}$ . The result is precisely  $\text{WRT}(g', \alpha') = \text{WRT}(g, \alpha)$ . Note that, at least in the case of the Fibonacci category, all of the relevant matrix entries can be stored and manipulated symbolically, so that no precision issues arise.

With the above polynomial-length certificate and polynomial-time verification algorithm, we have shown that the #P-hard Problem 3 lies in NP. This contradicts the assumption directly.  $\square$

#### ACKNOWLEDGEMENTS

CL was supported by Caltech’s Summer Undergraduate Research Thomas Lauritsen Fellowship, as well as by John Preskill with NSA/ARO grant W911NF-09-1-0442 and the Institute for Quantum Information and Matter (IQIM), an NSF Physics Frontiers Center with support from the Gordon and Betty Moore Foundation. Much of this work was completed while GA was a postdoctoral scholar at IQIM. GA was also supported by a Sapere Aude grant of the Danish Council for Independent Research, the ERC Starting Grant “QMULT” and the CHIST-ERA project “CQC”.

#### REFERENCES

- [1] Scott Aaronson and Alex Arkhipov. The computational complexity of linear optics. In *STOC’11—Proceedings of the 43rd ACM Symposium on Theory of Computing*, pages 333–342. ACM, New York, 2011.
- [2] Gorjan Alagic, Stephen P. Jordan, Robert König, and Ben W. Reichardt. Estimating Turaev-Viro three-manifold invariants is universal for quantum computation. *Physical Reviews A*, 82:040302, Oct 2010.

---

<sup>8</sup>The fact that the advice bitstring cannot be trusted may seem strange at first. It is helpful to think about the proof that 3SAT is in NP. In that case, it is obviously insufficient to demonstrate a polynomial-time algorithm that reads a formula and an advice bitstring, and then just accepts! The algorithm must check that the advice bitstring is a valid description of an assignment for the formula, and that the formula evaluates to true under that assignment.

- [3] Stephen A. Cook. The complexity of theorem-proving procedures. In *Proceedings of the Third Annual ACM Symposium on Theory of Computing*, STOC '71, pages 151–158, 1971.
- [4] Shawn X. Cui, Michael H. Freedman, and Zhenghan Wang. Complexity Classes As Mathematical Axioms II. [abs/1305.6076](#), 2013.
- [5] Christopher M. Dawson and Michael A. Nielsen. The Solovay-Kitaev algorithm. *Quantum Information & Computation*, 6(1):81–95, 2006.
- [6] Bill Fefferman. *The Power of Quantum Fourier Sampling*. PhD thesis, California Institute of Technology, Pasadena, California, 2014.
- [7] Michael H. Freedman. Complexity classes as mathematical axioms. *Annals of Mathematics*, 170(2):995–1002, 2009.
- [8] Michael H. Freedman, Alexei Kitaev, Michael J. Larsen, and Zhenghan Wang. Topological quantum computation. *American Mathematical Society. Bulletin. New Series*, 40(1):31–38, 2003.
- [9] Michael H. Freedman, Michael J. Larsen, and Zhenghan Wang. The two-eigenvalue problem and density of Jones representation of braid groups. *Communications in Mathematical Physics*, 228(1):177–199, 2002.
- [10] Sevag Gharibian, Yichen Huang, Zeph Landau, and Seung Woo Shin. Quantum hamiltonian complexity. [abs/1401.3916](#), 2014.
- [11] Joel Hass, Jeffrey C. Lagarias, and Nicholas Pippenger. The computational complexity of knot and link problems. *Journal of the ACM*, 46(2):185–211, March 1999.
- [12] Stephen P. Jordan and Gorjan Alagic. Approximating the Turaev-Viro invariant of mapping tori is complete for one clean qubit. In *Theory of Quantum Computation, Communication, and Cryptography - 6th Conference, TQC 2011, Madrid, Spain, May 24-26, 2011, Revised Selected Papers*, pages 53–72, 2011.
- [13] Robion Kirby and Paul Melvin. The 3-manifold invariants of Witten and Reshetikhin-Turaev for  $\mathfrak{sl}(2, \mathbb{C})$ . *Inventiones Mathematicae*, 105(3):473–545, 1991.
- [14] Robion Kirby and Paul Melvin. Local surgery formulas for quantum invariants and the Arf invariant. In *Proceedings of the Casson Fest*, volume 7 of *Geom. Topol. Monogr.*, pages 213–233. Geom. Topol. Publ., Coventry, 2004.
- [15] A. Yu. Kitaev, A. H. Shen, and M. N. Vyalyi. *Classical and quantum computation*, volume 47 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2002. Translated from the 1999 Russian original by Lester J. Senechal.
- [16] Bruce Kleiner and John Lott. Notes on Perelman’s papers. *Geometry & Topology*, 12(5):2587–2855, 2008.
- [17] Greg Kuperberg. How hard is it to approximate the jones polynomial? [abs/0908.0512](#), 2009.
- [18] Greg Kuperberg. Knottedness is in NP, modulo GRH. *Advances in Mathematics*, 256:493–506, 2014.
- [19] Leonid A Levin. Universal sequential search problems. *Problemy Peredachi Informatsii*, 9(3):115–116, 1973.
- [20] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.
- [21] Sergey Piunikhin. Reshetikhin-Turaev and Crane-Kohno-Kontsevich 3-manifold invariants coincide. *Journal of Knot Theory and its Ramifications*, 2(1):65–95, 1993.
- [22] V. V. Prasolov and A. B. Sossinsky. *Knots, links, braids and 3-manifolds*, volume 154 of *Translations of Mathematical Monographs*. American Mathematical Society, Providence, RI, 1997. An introduction to the new invariants in low-dimensional topology, Translated from the Russian manuscript by Sossinsky.
- [23] Kurt Reidemeister. Zur dreidimensionalen Topologie. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, 9(1):189–194, 1933.
- [24] N. Reshetikhin and V. G. Turaev. Invariants of 3-manifolds via link polynomials and quantum groups. *Inventiones Mathematicae*, 103(3):547–597, 1991.
- [25] Martin Scharlemann. Heegaard splittings of compact 3-manifolds. In *Handbook of geometric topology*, pages 921–953. North-Holland, Amsterdam, 2002.
- [26] Saul Schleimer. Polynomial-time word problems. *Commentarii Mathematici Helvetici. A Journal of the Swiss Mathematical Society*, 83(4):741–765, 2008.
- [27] James Singer. Three-dimensional manifolds and their Heegaard diagrams. *Transactions of the American Mathematical Society*, 35(1):88–111, 1933.

- [28] Morwen B. Thistlethwaite. A spanning tree expansion of the Jones polynomial. *Topology. An International Journal of Mathematics*, 26(3):297–309, 1987.
- [29] William P. Thurston. Three-dimensional manifolds, Kleinian groups and hyperbolic geometry. *American Mathematical Society. Bulletin. New Series*, 6(3):357–381, 1982.
- [30] V.G. Turaev and O.Y. Viro. State sum invariants of 3-manifolds and quantum 6j-symbols. *Topology*, 31(4):865 – 902, 1992.
- [31] Vladimir G. Turaev. *Quantum invariants of knots and 3-manifolds*, volume 18 of *de Gruyter Studies in Mathematics*. Walter de Gruyter & Co., Berlin, revised edition, 2010.
- [32] Dirk Vertigan. *The Computational Complexity of Tutte, Jones, Homfly and Kaufman invariants*. PhD thesis, Oxford University, Oxford, England, 1991.
- [33] Dirk Vertigan. The Computational Complexity of Tutte Invariants for Planar Graphs. *SIAM Journal on Computing*, 35(3):690–712, 2005.
- [34] Edward Witten. Quantum field theory and the Jones polynomial. *Communications in Mathematical Physics*, 121(3):351–399, 1989.

DEPARTMENT OF MATHEMATICAL SCIENCES, UNIVERSITY OF COPENHAGEN  
E-mail address: galagic@gmail.com

DEPARTMENT OF PHYSICS, MATHEMATICS AND ASTRONOMY, CALIFORNIA INSTITUTE OF TECHNOLOGY  
E-mail address: cwlo@caltech.edu